



The Cybersecurity Act: Countering Critical Security and Economic Threats

The threat to America's computer networks and the critical infrastructure they operate is grave and growing. Department of Defense information systems are probed millions of times every day by criminals, terrorists, and foreign intelligence organizations. Malicious cyberactors have repeatedly exploited vulnerabilities in government systems, and even companies that specialize in cybersecurity have been attacked. A successful cyberattack against our power grid, water systems, or financial networks could have a devastating impact on public safety and wreak havoc on our economy. To prevent a catastrophic attack, we must act now to bridge the security gaps that hinder our ability to defend against the evolving cyberthreat.

America's Critical Infrastructure is Vulnerable to Cyberattacks

- **America's power grids, communications lines and transportation systems are reliant on cyber networks.** Whether it is through unprotected connections between company systems to the Internet, or vulnerabilities within a company's control systems, America's critical infrastructure is dependent upon cyber networks that are vulnerable to attack.
 - As eight esteemed national security experts wrote to Senate Leadership, "The present cyber risk is shocking and unacceptable. Control system vulnerabilities threaten power plants and the critical infrastructure they support, from dams to hospitals." [[Letter from national security experts](#), 1/19/12]
 - Former Homeland Security Secretary Michael Chertoff notes, "[I]n an interconnected and interdependent world, the failure of one part of the network can have devastating collateral and cascading effects across a wide range of physical, economic and social systems." [Michael Chertoff Statement, 2/14/12, [letter here](#)]
- **Critical infrastructure networks are *already* under attack, and vulnerabilities are growing.** In just the past two years, cyberattacks on critical infrastructure in the U.S. have increased dramatically. In 2009, nine cyberattacks on critical infrastructure facilities were reported to the Department of Homeland Security (DHS). In 2011, that figure skyrocketed to 198 reported attacks. [[CNN Security Clearance](#), 7/4/12]

- **China is already studying the effects of attack-induced power failures in the U.S.** Backed by Chinese government money, a Chinese university published a study on the vulnerabilities of the U.S. power grid to cascade-based attacks and concluded, “attacks on nodes with the lower loads are more effective at creating cascading failures in the Western United States power grid than targeting higher capacity nodes.” *This study is just one of a number of other Chinese government sponsored studies analyzing vulnerabilities in the U.S. electric grid.* [[Northrop Grumman](#), 3/7/12]

Cyberattacks are a Dangerous National Security Threat

- **Our national security infrastructure is under constant attack.** The Department of Defense (DoD) is probed millions of times a day by malicious cyber actors. By September 2011, DoD had identified over 70 million cumulative malware threats against its networks. Foreign nations and intelligence organizations are working to exploit DoD’s networks and some have the capacity to disrupt elements of our information infrastructure. [[Testimony of Assistant Secretary Zachary Lemnios](#), 3/20/12; [DoD Strategy for Operating in Cyberspace](#), 7/11]
- **China and other entities are increasingly using cyberespionage against America.** A recent Northrop Grumman report concludes that, “Chinese capabilities in computer network operations... pose genuine risk to U.S. military operations in the event of a conflict.” Foreign states and terrorist organizations are constantly probing the U.S. defense grid, searching for state secrets and leaving behind malicious tools and weapons designed to go unnoticed and be surreptitiously activated later. These tactics allow groups to conduct reconnaissance and embed “sleeper” tools for later use during a conflict. [[Northrop Grumman](#), 3/7/12; [AOL Defense](#), 3/21/12]
- **Cyberattacks have been recognized as an extremely serious threat.** DoD experts have identified cyberattacks as, “one of the most serious national challenges to security.” Inadequate defense of cyberspace is the nation’s most serious vulnerability, and threatens both the country’s national security and economic prosperity. [[DoD Strategy for Operating in Cyberspace](#), 7/11]

Cyberattacks Weaken the American Economy

- **Intellectual property theft represents “the greatest transfer of wealth in history.”** General Keith Alexander, Director of the National Security Agency (NSA), has noted that the effects of this theft on American industry are extensive and economically devastating. Echoing that, James Lewis from CSIS testified, “Because of the ease of cyber espionage, our national spending on innovation is, in effect, a partial subsidy to foreign competitors: they share the fruits of our investments without having to pay for them.” [[Foreign Policy](#), 7/9/12; [Testimony of James Lewis](#), 2/16/12]
 - “Economic espionage inflicts costs on companies that range from loss of unique intellectual property to outlays for remediation, but no reliable estimates of the monetary values of those costs exist. Many companies are unaware when their sensitive data is pilfered, and those that find out are often reluctant to report the loss, fearing potential damage to their reputation.” [[NCIX report to Congress](#), 10/11]

- **Cyber incidents cost American industries billions of dollars every year.** According to a Norton study, cybercrime cost the U.S. \$32 billion in cash and an additional \$108 billion in time over a recent twelve month period. The worldwide economic impact of cybercrime is even more staggering. According to the report, “With 431 million adult victims globally in the past year and at an annual price of \$388 billion globally based on financial losses and time loss, cybercrime costs the world significantly more than the global black market in marijuana, cocaine and heroin combined (\$288 billion).” Other estimates have placed the cost of cybercrime to the global economy at more than \$1 trillion each year. [[Symantec](#), 9/7/11; [Symantec](#)]
- **“Cyber espionage means fewer American jobs.”** A recent report by Northrop Grumman on China’s cyber activities found that, “Professional state sponsored intelligence collection ... increasingly is being used to collect economic and competitive data to aid foreign businesses competing for a market share with their U.S. peers.” Improved cybersecurity practices could go a long way in protecting Americans’ trade secrets and safeguarding the country’s economic prosperity. [Former U.S. Secretary of Commerce John Bryson, [Politico](#), 3/8/12; [Northrop Grumman](#), 3/7/12]
- **Foreign economic competitors are using cyberespionage to steal intellectual property and put American businesses out of work.** Businesses invest a great deal of capital to develop new products, and having their intellectual property stolen by competitors can be devastating, leading to layoffs, slowed hiring, and a weakened economy.
 - “Over the past five years, a highly sophisticated team of operatives have stealthily infiltrated more than 70 U.S. corporations and organizations to steal priceless company secrets.... robbing companies of the ideas that are the source of American ingenuity.... In the aggregate, the theft of this property, including everything from sensitive defense technology to innovative industrial designs, insidiously erodes government and corporate competitive advantages among global peers. [Former U.S. Secretary of Commerce John Bryson, [Politico](#), 3/8/12]

American Consumers are at Risk of Being Victimized by Cyberattacks

- **Individuals can be the targets of malicious cyberattacks.** Stewart McClure, Executive Vice President of leading computer security firm McAfee, recently testified, “The threats that individuals and consumers face run the gamut from identity theft to loss of financial or personal information, to infection of their systems and destruction of hardware, software and data. The advent of new mobile technology, particularly smartphones and tablets, has opened up new attack vectors for hackers.” [[Testimony of Stuart McClure](#), 4/24/12]
 - In 2010, over 11 million American adults were the target of identity fraud, costing them more than \$54 billion. [[Javelin Strategy](#), 2/10/10]
 - The Department of Justice’s Internet Crime Complaint Center received almost 315,000 crime complaints in 2011. The loss associated with these complaints exceeded \$485 million. [[Internet Crime Complaint Center](#), 2011]
 - According to one privacy watchdog, almost 550 million sensitive records – including social security numbers, passwords, and credit card numbers – have been breached in the U.S. alone since 2005. [[Privacy Rights Clearinghouse](#), 12/16/11]

- **Private computers are at particular risk.** A recent survey by computer security firm McAfee found that one out of every six private U.S. computers has no basic security protections in place at all. Many falsely believe that by visiting only “safe” and well-known websites, their computers and mobile devices are secure, but the facts say otherwise. According to a Norton study, “Every second 14 adults become a victim of cybercrime, resulting in more than one million cybercrime victims every day.” [[McAfee](#), 5/29/12; [Symantec](#), 9/7/11]